Network Reachability In Cross Domain Using Privacy Preserving Protocol

S.Lavanya [1], Lithiya Sara Babu[2] , S.Seetha[3]

Abstract— **The importance for detecting violations of security policies across the network and understanding end-to-end network behavior is by network reachability the upcoming browser-to-browser communication services present problems for user discovery in end –to-end mode. There are many difficult problems for performing the computation across the networks, and also for the privacy of security policies. For this problem, we propose an effective privacy preserving protocol for cross domain network reachability. Our privacy preserving protocol represents Access Control List (ACL) rules for determine the network reachability and also preserving privacy policy. This Protocol determines network reachability accurately along a network path with different administrative domains. We have to evaluated and implemented PPB protocol in synthetic and real ACLs. In the case of large enterprise networks also we have to implement this protocol.**

Keywords — Cross domain, network reachability, privacy preserving.

I. INTRODUCTION

Preserve the privacy of network configuration information belongs to different domains The main purpose of end to end network traversing and detecting security polices by network reachability. To quantify this end-end network traversing is more difficult because it has many reasons dynamic routing network address translation (NAT), Access Control Lists (ACLs), have been deployed on network devices for to difficult network reachability.

Therefore, to perform an exact analysis, the administrators collect all the traversing information from these types of network devices. Collecting some information is very difficult due to the privacy and security concerns. The explosion of the internet has occurred due to an increase in the complexity and advanced features of these devices, thus, making reachability analysis computationally expensive and error-prone. The network reachability is one of the main reasons in the monitoring of end to end behavior of the network and identifying the detecting violation of policies of security. To calculate the network reachability using privacy preserving protocol of access control list. The limitation is when new links are added to the network that a time it will not work properly. But it is very efficient secure and fast communication overhead. Multiple administrators is more difficult to accessing the network reachability.

The Domain Name Service (DNS) is, in fact, a well established discovery service. It maps domain names to IP addresses of the actual endpoints. The DNS queries are served by a local resolver on the DNS server in the same domain. If the address cannot be resolved locally, the query is resolved by iteratively contacting the authoritative servers for the domain in a hierarchical way. The DNS is well governed, but its reliance on extensive caching results in delays in the propagation of new entries or updates. To enhance performance, DNS dynamically updates domain names as well as network reachability may entirely a large for many networks because of to high complexity and the small level percentage of advanced reachability debugging tools, its a reality. in first case is more difficult for network assembling then the skilled network operators can exactly maintain The complexity of modern networks has been rapidly increasing due to the explosive growth of Internet connectivity expanding from end-hosts to pervasive devices and network-supported applications of various scales. the second one is due to the lack of advanced network reachability debugging tools.

i) MONITORING NETWORK SECURITY:

To Verifying that the failed ACLs satisfy some security specifications is an integral part of network security monitoring and auditing. The current practice is to send particular packets.The main drawback of this protocol is that when the new domains are added in the network the protocol will not work properly. Because the protocol is started with the pre-processing work i.e. creation of access control lists for each domain. So when added the domains once it started then it cannot do pre-processing. So it will fail.

ii) Cross Domain Network Reachability

Cross domain is in the sense of information assurance and will be provide an ability to statically or dynamically access information to transfer between different security domains. Network reachability is one of the network path from the source station to the destination station it is defined as the set of packets that are allowed by all network devices on the single path. At the time of network reachability traversing is important for understanding end-to-end network behavior and detecting the violation of security policies.

iii) PRIVACY-PRESERVING PROTOCOL

From Figure 1: privacy preserving part of the protocol issued to control the level of sharing and protect the secure data from being disclosed, and the similarity part issued to resolve the different notations that refer to the same entity.

i) Enables Host 1 to validate the reachability to Host 2 by computing $MM(TT3) \cap MM(TT4)$, since $MM\ TT1 \cap MM\ TT2 = MM(TT3)$ is known by Host 1

ii)No domain can reveal the admitted traffic T of other domains.

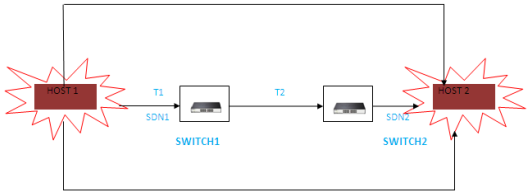

Figure 1: Privacy Preserving Protocol

II. Related Work

A Quantitative study of firewall configuration errors Computer used Once a company acquires a firewall a systems administrator must configure and manage it according to security policy that meets the company's needs. Configuration is a crucial task probably the most important factor in the security a firewall provides. The Algorithmic Security is used a network security company that he cofounded. The limitations are Plug flow reactors have a high volumetric unit conversion, run for long periods of time without maintenance and the heat transfer rate can be optimized by using thinner or thicker tubes in parallel. Main importance of Continuous Stirred Tank Reactor are normally of different equations and also in kinetics of the reaction being taken and will go to some extent determine which system should be used.

Efficient private matching and set present protocols based on the use of ho- mom orphic encryption and balanced hashing,[2] for both semi-honest and malicious environments. For lists of length k, obtain O(k) communication overhead and O(k ln ln k) computation. In the case of semi environment a secured protocol is set for all standard model, thus malicious environment is secure in the random oracle model. The computing exponentiations algorithm is used. The limitations are immaturity, Reliance on third-party illuminators, Complexity of deployment. The advantages are Lower procurement cost, Lower costs of operation and maintenance, due to the lack of transmitter and moving parts , Covert operation, including no need for frequency allocations.

In firewall design, completeness, consistency and compactness all are often placed at the entrance of each private net work in the Internet. The main function of a firewall is to check whether each packet that transfers through the entrance and decide whether to accept the packet and allow it to proceed or to discard the packet. Are wall is usually designed as a sequence of rules. FDD algorithm is used. The limitations are all logics are for representing proofs, including propositional logic. Larger order of the logic is more powerful and it is in the sense of its language being more expressive and its deduction being more general. The Advantages are Less powerful logic is that it is easier to reason about, and that it is tends to be easier to write algorithms for, in the sense that (depending on what the algorithm is intended to do) these algorithms will tend to be more complete and/or efficient and/or to terminate (e.g. algorithms for proving statements in the logic). To maintain the advantage of more powerful logic is that it is more costly and thus able to representing and/or proving more of mathematics.

According to the architecture of enterprise networks connectivity, our today's enterprise networks is regulated and complex routing and policies along with various mechanism such as ACLs that attempt to retrofit access control onto an otherwise permissive network architecture. These enterprise network leads to inflexible, fragile, and difficult to manage. MST algorithm has the property has no switch learns the network topology nor is the topology reproducible from packet traces uses little power, has no fragile moving parts, and for most capacities is small and light. Data must be stored in flash drives must be in mechanical shock, magnetic fields, dust.

Designs in structured firewall may addresses the problem of completeness because of syntactic requirements in the decision diagram force of the firewall to consider different traffic. It also addresses the compactness problem because in the second step we use two algorithms (namely FDD reduction and FDD marking)[4] to combine rules together, and one algorithm (namely firewall compaction)to remove redundant rules. Moreover, the techniques and algorithms presented in this paper are extensible to other rule-based systems such as IP sec rules. Distance vector algorithm is used. The advantage of such representation will become evident when combining several IDDs. The main problem with fuzzing to find program faults is that it generally only finds very similar.

Privacy- preserving cross- domain network reachability quantification have implemented and evaluated our protocol on both real and synthetic ACLs. The experimental results show that the online processing time of an ACL with thousands of rules is less than 25 seconds; the comparison time of two ACLs is less than 6 seconds and the communication cost between two ACLs with thousands of rules is less than 2100 KB. The Pohlig-Hellman algorithm. this algorithm is used. The Advantages are Streamlines the supply chain from point of origin to point of sale. Reduces labour costs through less inventory handling. The Limitations are Potential partners may not have the necessary storage capacities. An adequate transport fleet is needed to operate.

Efficient and secure protocols for privacy-preserving set operations The Fast one secure against the active adversary. Our constructions of NIZK [1] have independent interest in that, though also mentioned as building blocks, the previous work did not illustrate how to construct them. We construct these NIZK with an additional non-malleable property, the same complexity as claimed in the previous work, and also an improvement on the communication complexity.

The Algorithms are Probabilistic Polynomial-Time is algorithm is used. One advantage of is that we no longer need the two extra initial messages. The Limitations are Migration addresses the possible obsolescence of the data carrier, but does not address the fact that certain technologies which run the data may be abandoned altogether, leaving migration useless.

In Privacy-preserving cooperative firewall will optimized this paper to explore and inters firewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. In this paper, we propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. The Advantages are Malicious activity may be identified by the other party using anomaly detection Approaches.

It avoids encrypting and sending the duplicate prefixes for each field and, hence, significantly reduces the computation and communication costs. The Disadvantages are No corrupted employees are trying to reveal the private firewall policies of other parties. Condition holds for all the predicates computed from rule r and then rule r is redundant.

III. System Architecture

From the architecture in Figure:2 the login phase consist of admin login and user login , in the section of admin login we have to create a domain to transfer data and to also to upload file and set the privilege data to the domain. The admin have the full authority to view or delete or download the file from server. In user login section each user is provided with a secret key to access the file .Each user can change their data according to the data being saved in the database. Once user enters into system, user must enter a correct key to access the selected file in database. If the key is correct then the user can view or download the file. If the key is incorrect user can't access the file.

By viewing the file we have to ensuring privacy, file has being encrypted and decrypted according to the usage. Firewall protection of cross domain protocol must be ensuring here. For more effective and secured data will be accessed by the user.

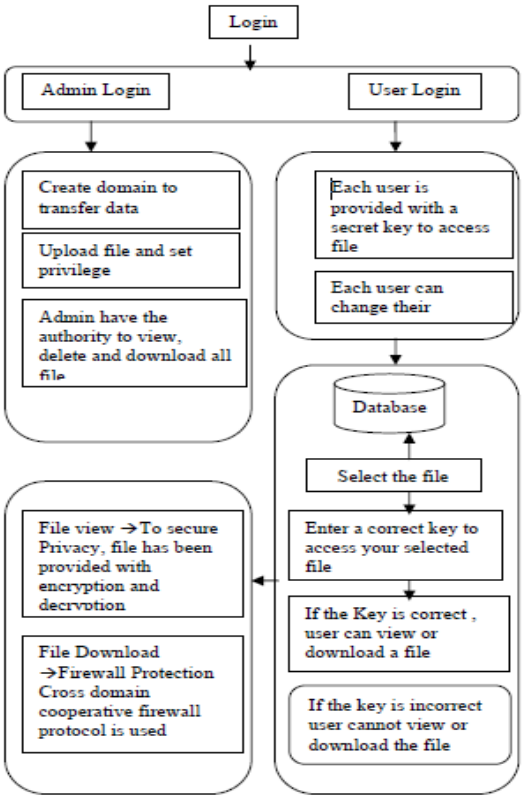

Figure.2 System Architecture

IV. Proposed Work.

MODULE DESCRIPTION

- Extended ACL pre-processing
- Extended ACL encoding and encryption
- ACL comparison
- Optimization

A. Extended ACL pre-processing

In the phase of Extended ACL pre-processing module, we have to convert Extended-ACLs into its equivalent representation and protection based firewall decision diagram. It must be most effective and also extract data from the non-overlapping rules decisions.

B. ACL encoding and encryption

In the phase of encoding and encryption we have to perform privacy-preserving comparison for the reduction of problems occur in the time of computing privacy-preserving intersection of two numerical ranges. By the transformation of rules in first, we have to represent the ranges into a sequence of prefix numbers and also used to encrypt these numbers with different parties of secret keys.

By the help of this phase we have to enable the computation of intersection of ACL in different parties without overlapping rules or revealing the rules.

C. ACL comparison

In the comparison module ACL computes the destination of intersection of its non overlapping rules with the rules from its adjacent ACL. Then the adjacent ACL repeats the computation process with its adjacent ACL until the source ACL is reached.

D. Optimization

At the last stage of collaboratively decryption in ACL the encrypted intersection of the non overlapping rules, but only the first party (with the source ACL) obtains the result. To reduce the computation and communication cost, we use the divide-and-conquer strategy to divide the problem of computing reach ability of ACLs to the problem of computing reach ability of three ACLs. The initial intersection is performed among the rules of three adjacent ACLs that are located in a sequence along the network path. Subsequent comparisons are grouped in a similar manner, i.e., the intersection of three ACLs can be treated as a new ACL, and the process is repeated among three new ACLs. This optimization technique reduces the number of ACL encryptions and the number of messages in our protocol from O(n2)to O(n).

V. CONCLUSION

Firewalls are designed to provide access control. The Cross Domain method is to cooperative the firewall across different domain administrative by the usage of key management in the order of privacy preserving and security policies. In this method the security will be improved and it must be controlled and also can be able to provide privacy. Need to check Privacy-Preserving Range Comparison. If the rule exists. Propose a cross domain cooperative firewall protocol to optimize the network. If the rule does not exist, the network performance collapse and discards due to the entry of third party. Thereby privacy and security fails. To overcome this bug underwent a study of cross domain cooperative firewall protocol. To implemented protocol in java and conducted extensive evaluation. As a result of real firewall policies the required protocol may avoid 98% of rules in firewall.

REFERENCES

[1]. B. Zhang, T. S. E. Ng, and G. Wang, "Reachability monitoring and verification in enterprise networks," presented at the SIGCOMM, 2008(poster).

[2]. Kyle Ingols, Richard Lippmann, Keith Piwowarski "Practical Attack Graph Generation for Network Defense".

[3]. P. Matousek, J. Rab, O. Rysavy, and M. Sveda, "A formal model for network-wide security analysis," in Proc. *IEEE Int. Conf. Workshop Eng. Comput. Based Syst.*, 2008, pp. 171–181.

[4]. Erich Ortner, "Temporal and Modal Logic Based Event Languages for the Development of Reactive Application Systems" July 24, 2003

[5]. Alex X. Liu, Member, IEEE, and Amir R. Khakpour "Quantifying and Verifying Reachability for Access Controlled Networks" *IEEE/ACM TRANSACTIONS ON NETWORKING,* VOL. 21, NO. 2, APRIL 2013

[6]. Martin Casado, Tal Garfinkel, Aditya Akella, Michael J. Freedman, "SANE: A Protection Architecture for Enterprise Networks".

[7]. Franck Le, Sihyung Lee, Student Member, *IEEE, Tina Wong, Hyong S. Kim, and Darrell Newcomb, "Detecting Network-Wide and Router-Specific Misconfigurations Through Data Mining" IEEE/ACM TRANSACTIONS ON NETWORKING,* VOL. 17, NO. 1, FEBRUARY 2009.

[8]. Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu "Cross-Domain Privacy-Preserving Cooperative Firewall Optimization" *IEEE/ACM TRANSACTIONS ON NETWORKING,* VOL. 21, NO. 3, JUNE 2013.

[9]. Alex X. Liu, "Privacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Networks" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,* VOL. 22, NO. 5, MAY 2011.

[10]. M. G. Gouda and A. X. Liu, "Firewall design: Consistency, completeness and compactness," in Proc. ICDCS, 2004, pp. 320–327.

[1]**S.Lavanya B.E, M.E.,** Assistant Professor, Department of Computer Science and Engineering, Karur College of Engineering, Karur**.**

,
[2]**Lithiya Sara Babu B.Tech, M.E.,** Assistant Professor, Department of Computer Science and Engineering, Karur College of Engineering, Karur**.**

[3]**S.Seetha B.E, M.E.,** Assistant Professor, Department of Computer Science and Engineering, Karur College of Engineering, Karur**.**